



<b>DEPARTMENT:</b> NC DHHS Privacy and Security Office	<b>POLICY NAME:</b> ZixMail Usage Policy
<b>PAGE:</b> 1 of 2	<b>REPLACES POLICY DATED:</b> None
<b>EFFECTIVE DATE:</b>	<b>ORIGINAL EFFECTIVE DATE:</b>
<b>REVISED DATE:</b>	<b>APPROVED DATE:</b>
<b>APPROVED BY:</b> Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

**SCOPE:**

To provide a framework for the usage of ZixMail within the North Carolina Department of Health and Human Services (NC DHHS)

**PURPOSE:**

The purpose of this policy is to identify the required use of ZixMail in conducting official NC DHHS business via email

**POLICY:**

To ensure compliance with HIPAA and other federal, department and state regulations and standards, any sensitive data, internal proprietary and confidential data must be secured using approved encryption technologies when transmitted electronically.

ZixMail is the email encryption tool employed by NC DHHS to ensure that official email communication containing confidential and/or sensitive information is secure and encrypted end-to-end between the sender and intended recipient(s). Confidential data includes, but is not limited to:

- Protected Health Information (PHI)
- Personally, Identifiable Information (PII)
- Internal Revenue Service (IRS) data
- Payment Card Industry (PCI)
- Internal proprietary documents
- Trade secrets, design documents

The Department intends ZixMail to be used for sending emails that contain sensitive and/or confidential information.

The primary purpose of email is to accomplish day to day NC DHHS business (general, operational, programmatic, and administrative). All emails sent via the NC Email system are subject to Public Records Requests, so personal or non-business-related communications should not be sent using the department email system. To facilitate the integrity and confidentiality of an email and its attachments, ZixMail must be used. ZixMail ensures the data is protected end-to-end in transit, meets federal, state and department requirements, and protects the integrity of data and emails for any public records requests.

There can be instances where it is determined that, due to the sensitivity of the data, email



<b>DEPARTMENT:</b> NC DHHS Privacy and Security Office	<b>POLICY NAME:</b> ZixMail Usage Policy
<b>PAGE:</b> 2 of 2	<b>REPLACES POLICY DATED:</b> None
<b>EFFECTIVE DATE:</b>	<b>ORIGINAL EFFECTIVE DATE:</b>
<b>REVISED DATE:</b>	<b>APPROVED DATE:</b>
<b>APPROVED BY:</b> Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary IT Operations	

may not be an appropriate method used to transmit highly sensitive data. This can include IT system development code, application deployment/system testing reports, program/system certification, etc. In these instances, alternative communication channels should be used which can include, but would not be limited to alternative channels that:

- have specific communication capabilities such as web portals
- use Secure File Transfer Protocol (SFTP) that meets state and federal encryption and password requirements

When the state and vendors agree that communication related to these types of contracts/agreements is specific and sensitive enough to establish alternative channels, these alternative channels must be used rather than department email.